Notice of Allowability	Application No.	Applicant(s)	
	09/578,215	BODEN ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment dated 03/30/06*.

2. ☒ The allowed claim(s) is/are *1-4, 6-10, 12, and 16-22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

HOSUK SONG
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Shelley M. Beckstrand on June 12, 2006.

In the claims:

Please canceled claims 5, 11, and 13-15.

Please replace claims 1, 4, 6, 8, 12, and 16-21.

Claim 1. [Currently amended] A method of operating a virtual private network (VPN) based on [[IP sec]] IPsec that integrates network address translation (NAT) with [[IP sec]] IPsec processing, comprising the steps executed at one end of a VPN connection of:

configuring a VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine;

configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

starting said VPN connection;

loading to an operating system kernel at said one end of said VPN connection the security associations and connection filters for said VPN connection;

processing at said one end of said VPN connection a IP datagram for said VPN connection;

applying VPN NAT at one end of said VPN connection to said IP datagram with source and destination port values after the application of VPN NAT being the same as before application of VPN NAT[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]] internet key exchange protocol (IKE) [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

Claim 4 [Currently Amended] The method of claim 1, further for integration of NAT with IP Sec for manually-keyed [[IP sec]] IPsec connections, comprising the further step of manually configuring connection keys.

Claim 5. [Canceled] ~~The method of claim 1, further for integrating NAT with [[IP sec]] IPsec for dynamically keyed (e.g. IKE) [[IP sec]] IPsec connections, comprising the further step of:~~

~~configuring the VPN connections to obtain their keys automatically.~~

Claim 6. [Currently Amended] The method of claim 1, further for integrating NAT with [[IP sec]] IPsec Security Associations, negotiated dynamically by [[(e.g.IKE)]] internet key exchange protocol (IKE), wherein said starting step further comprises creating a message for IKE containing said IP address from said NAT pool; and further comprising the step of operating IKE to obtain dynamically negotiated keys.

Claim 8. [Currently amended] A computer implemented method for allowing the definition and configuration of NAT directly with definition and configuration of IPsec-based VPN connections and VPN policy, comprising the steps executed by a digital processor at one end of a VPN connection of:

configuring at one end of said VPN connection the requirement for VPN NAT by a yes/no decision in a policy database for each of the three types of VPN NAT, said three types being VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT;

[[and]]

configuring at said one end of said VPN connection on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine a remote IP address pool or a server IP address pool selectively responsive to said yes/no decision for each said VPN NAT type; and upon subsequent start of said VPN connection, processing inbound and outbound packets at said one end of said VPN connection responsive to configuration of said VPN NAT in said policy database and configuration of said remote IP address pool[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically..

Claim 11. [Currently amended] ~~A computer implemented method of providing customer tracking of VPN NAT activities as they occur in an operating system kernel, comprising the steps executed at one end of a VPN connection of:~~

~~responsive to VPN connection configuration, generating journal records as a log entry in a file system of an operating system at said one end of said VPN connection;~~

~~updating at said one end of said VPN connection said journal records with new records for each datagram processed through a VPN connection; and~~

~~enabling a customer to manage said journal records.~~

Claim 12. [Currently amended] A computer implemented method of allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing, comprising the steps executed by a digital processor at one end of a VPN connection of:

configuring at said one end of said VPN connection a server VPN NAT IP address pool for a system being configured;

storing at said one end of said VPN connection specific IP addresses that are globally routable in said server VPN NAT IP address pool;

configuring at said one end of said VPN connection a VPN connection to utilize said server VPN NAT IP address pool; and

managing at said one end of said VPN connection total volume of concurrent VPN connections responsive to the number of addresses in said server VPN NAT IP address pool with source and destination port values before and after application of VPN NAT being the same[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

Claim 13. [Canceled] ~~A method of controlling the total number of VPN connections for a system based on availability of VPN NAT addresses, comprising the steps executed at one end of a VPN connection of:~~

~~configuring on a VPN gateway machine at said one end of said VPN connection employing only IP address data available at said VPN gateway machine the totality of remote IP address pools with a common set of IP addresses, said addresses being configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses; and~~

~~limiting at said one end of said VPN connection the successful start of concurrently active VPN connections responsive to the number of said IP addresses configured across the totality of said remote address pools.~~

Claim 14. [Canceled] ~~A method of performing virtual private network (VPN) network address translation on selected ICMP datagrams, comprising the steps executed at one end of a VPN connection of:~~

~~combining at said one end of said VPN connection [[IP sec]] IPsecurity & VPN NAT by detecting selected types of ICMP type packets; and~~

~~responsive to said selected types, performing at said one end of said VPN connection network address translation functions on the entire datagram including ICMP data.~~

Claim 15. [Canceled] ~~A method of performing virtual private network (VPN) network address translation on selected FTP datagrams, comprising the steps executed at one end of a VPN connection of:~~

~~combining at said one end of said VPN connection [[IP sec]] IPsecurity & NAT by detecting the occurrence of FTP PORT or PASV FTP commands; and~~

~~responsive to said command, performing at said one end of said VPN connection network address translation on the FTP data and the header.~~

Claim 16. [Currently amended] A computer system for operating a virtual private network (VPN) based on [[IP sec]] IPsec that integrates network address translation (NAT) with [[IP sec]] IPsec processing executed by a digital processor at one end of a VPN connection, comprising:

means for configuring on a VPN gateway machine at said one end of a VPN connection a VPN NAT IP address pool employing only IP address data available at said VPN gateway machine;

means for configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

means for obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

means for starting said VPN connection at said one end of said VPN connection;

means for loading at said one end of said VPN connection to an operating system kernel the security associations and connection filters for said VPN connection;

means for processing at said one end of said VPN connection a IP datagram for said VPN connection; [[and]]

means for applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after application of VPN NAT being the same as before application of VPN NAT[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically

Claim 17. [Currently amended] A system for definition and configuration of NAT directly with definition and configuration of VPN connections and VPN policy executed by a digital processor at one end of a VPN connection, comprising:

Computer readable-medium embodying a policy database for configuring at said one end of said VPN connection the requirement for VPN NAT by a yes/no decision for each of the three types of VPN NAT, said three types being VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT; and

a remote IP address pool or a server IP address pool at said one end of said VPN connection selectively configured on a VPN gateway machine at said one end of a VPN connection responsive to said yes/no decision for each said VPN NAT type employing only IP address data available at said VPN gateway machine [[.]];

upon subsequent start of said VPN connection, processing inbound and outbound packets at said one end of said VPN connection responsive to configuration of said VPN NAT in said policy database and configuration of said remote IP address pool; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically

Claim 18. [Currently amended] A system implemented at one end of a VPN connection for allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing, comprising:

a server VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection configured for a given system being configured for containing multiple ~~address~~ addresses configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses employing only IP address data available at said VPN gateway machine;

said server VPN NAT IP address pool storing specific IP addresses that are globally routable;

a VPN connection at said one end of said VPN connection configured to utilize said server VPN NAT IP address pool; and

a connection controller for managing at said one end of said VPN connection total volume of concurrent VPN connections responsive to the number of addresses in said server VPN NAT IP address pool with source and destination port values after application of VPN NAT being the same as before application of VPN NAT[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

Claim 19. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps executed at one end of a VPN connection for operating a virtual private network (VPN) based on [[IP sec]] IPsec that integrates network address translation (NAT) with [[IP sec]] IPsec processing, said method steps comprising:

configuring on a VPN gateway machine at said one end of a VPN connection a NAT IP address pool employing only IP address data available at said VPN gateway machine;

configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

obtaining a specific IP address from said VPN NAT IP address pool, and

allocating at said one end of said VPN connection said specific IP address for said VPN connection;

starting said VPN connection at said one end of said VPN connection;

loading to an operating system kernel at said one end of said VPN connection the security associations and connection filters for said VPN connection;

processing at said one end of said VPN connection a IP datagram for said VPN connection; and

applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after application of VPN NAT being the same as before application of VPN NAT[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

Claim 20. [Currently amended] An article of manufacture comprising:

a computer useable medium having computer readable program code means embodied therein for operating a virtual private network (VPN) based on [[IP sec]] IPsec that integrates network address translation (NAT) with [[IP sec]] IPsec processing executed at one end of a VPN connection, the computer readable program means in said article of manufacture comprising:

computer readable program code means for causing a computer to effect configuring a VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine;

computer readable program code means for causing a computer to effect configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

computer readable program code means for causing a computer to effect obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

computer readable program code means for causing a computer to effect starting at said one end of said VPN connection said VPN connection;

computer readable program code means for causing a computer to effect loading at said one end of said VPN connection to an operating system kernel the security associations and connection filters for said VPN connection;

computer readable program code means for causing a computer to effect processing at said one end of said VPN connection a IP datagram for said VPN connection; and

computer readable program code means for causing a computer to effect applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after the application of VPN NAT being the same as before application of VPN NAT[[.]]; and

further for integrating NAT with [[IP sec]] IPsec for dynamically-keyed [[(e.g.IKE)]], internet key exchange protocol (IKE), [[IP sec]] IPsec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

Claim 21. [Currently amended] A computer implemented method for providing IP security in a virtual private network using network address translation (NAT), comprising the steps executed by a digital processor at one end of a VPN connection of:

dynamically generating at said one end of said VPN connection NAT rules and associating them selectively with manual and dynamically generated [[(e.g.IKE)]], internet key exchange protocol (IKE), Security Associations, comprising the further step of:

configuring the VPN connections to obtain their keys automatically; thereafter

beginning at said one end of said VPN connection IP security that uses the Security Associations; and then

as [[IP sec]] IP security is performed on outbound and inbound datagrams, selectively performing at said one end of said VPN connection one or more of VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT on said outbound and inbound datagrams[[.]], so as to provided said IPsec for communication conducted in said VPN.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Linh LD Son
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER